Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A system with a local application entity and communications means by which the local application entity can exchange application messages with peer remote application entities on other systems, the communication means including a transport entity for providing transport services, and a security entity logically positioned above the transport entity and operative to set up secure communication sessions with peer security entities in other systems for the passing of application messages in protocol data units (PDUs) exchanged between the security entities, the security entity including a tunnelling mechanism for establishing a tunnel through an access-controlling intermediate system whereby to enable the local application entity to exchange application messages securely with a remote application entity on another system reachable via said intermediate system, the tunnelling mechanism being arranged to establish this tunnel by first setting up a first security session with said intermediate system and then a nested, second, security session with said another system with second PDUs associated with the second session being encapsulated as payload within first PDUs associated with the first session; and each first PDU comprising addressing information, payload, and a message-type field for indicating to the security entity in the intermediate system whether a said first PDU it receives encapsulates a said second PDU that is to be extracted and sent on or whether it holds data for use by the intermediate system.

2. (previously presented) A system according to claim 1, wherein each second PDU has a destination address which is modifiable without invalidating any security processing applied specifically to that PDU whereby the intermediate system can redirect second PDUs that are indicated by the message type of an encapsulating first PDU as intended for sending on.

3. (original) A system according to claim 1, wherein each security session is between specified application entities and the establishment of a security session is effected through a handshake process between the security entities concerned during which each application entity involved is required to show, by attribute certificates exchanged between the security entities, that it possesses certain attributes required of it by the other application entity.

4. (original) A system according to claim 3, wherein a remote broker system runs a broker application that fronts for a target application entity that the local application entity wishes to contact, the security entity of the local application entity being initially operative to seek to establish a security session with the broker application as said target application entity requiring of the broker application attributes considered by the local application entity as appropriate for the target application, the broker application responding by causing its associated security entity to return as part of its handshake with the security entity of said local application, an indication that the broker application is a relay for the target application entity, the local application entity being thereupon operative to decide whether to request a tunnel be set up

through the broker system by the tunnelling mechanism and if so what attribute requirements must now be met by the broker application.

5. (original) A system according to claim 1, wherein a remote broker system runs a broker application that fronts for a target application entity that the local application entity wishes to contact, the security entity of the local application entity being initially operative to seek to establish a security session with the broker application as said target application entity, the broker application responding by causing its associated security entity to return to the security entity of said local application, an indication that the broker application is a relay for the target application entity, the local application entity being thereupon operative to decide whether to request a tunnel be set up through the broker system by the tunnelling mechanism and if so what attribute requirements must be met by the broker application.

6. (original) A system according to claim 1 wherein said tunnelling mechanism is capable of setting up multiply-nested security sessions for tunnelling through a corresponding number of intermediate systems.

7. - 8. (cancelled)

9. (currently amended) A method of communication between local and remote systems via an intermediate system, each system including a transport entity providing transport services, and a security entity logically positioned above the transport entity

for setting up secure communication sessions with peer entities; the method comprising:

the local entity establishing first and second secure communication sessions respectively with the intermediate system and the remote system with second protocol data units (PDUs), associated with the second secure session being encapsulated as payload within first PDUs associated with the first secure session that each comprise addressing information, a type indicator, and said payload, and

the intermediate system using said type indicator to determine whether a first PDU it receives encapsulates a second PDU or whether it holds data for use by the intermediate system.